テロ対策ネットワーク岐阜通信

サイバー空間の脅威と対策

本年９月に、警察庁が、令和３年上半期におけるサイバー空間をめぐる脅威の情勢等を発表しました。発表によると

○　ランサムウェア※1による被害が大幅に増加

○　サイバー攻撃による情報流出事案が多数発生

するなど、サイバー空間における脅威は、今も極めて深刻な情勢が続いています。

１　ランサムウェア被害件数

令和３年上半期　企業、団体等におけるランサムウェア被害で、都道府県警察から警察庁に報告のあった件数

61 件（昨年下半期比＋40 件）

２　被害の特長

(1)　二重恐喝による被害が多く占める

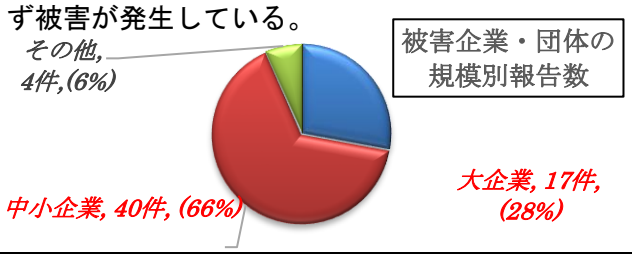
○　被害件数(61 件)のうち、金銭の要求手口を確認できた被害は 35 件。

○　このうち二重恐喝※2の手口によるものが 27 件。

○　暗号資産による直接金銭の要求があった被害は 29 件。

(2)　企業・団体の規模を問わない

被害企業の内訳を被害企業・団体の規模別にみると大企業 17 件、中小企業 40 件で、規模を問わず被害が発生している。



(3)　復旧に時間と費用が必要

○　復旧に要した期間は、１週間以内が最も多かったが、なかには

２ヶ月以上要した

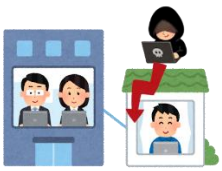
ものもあった。

○　調査・復旧費用の総額に

1000万円以上の経費

を要したものが15件で、全体の39%を占めている。（全回答39件）

(4)　感染経路



感染経路は、

・　VPN 機器※3

・　リモートデスクトップ

からの侵入が８割近くを占めるなど、テレワーク等の普及を利用して侵入したと考えられるものが多数を占める。

※１　感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム

※２　ファイル暗号化による身代金要求に加え、暗号化前に窃取したファイルを公開すると脅迫し身代金を要求するもの

※３　一般的なインターネット回線を利用して作られる仮想のプライベートネットワーク「VPN」を導入するための機器。VPN の利用により、トンネリング・暗号化・承認等を設定し、外部から通信内容が読み取れないように通信網が構築される

３　ランサムウェア被害を防ぐために

(1) 被害防止対策

○　電子メール等への警戒

添付ファイル付きのメールやリンク付きのメールについては、送信元への確認を行うなどその真偽を確認し、不用意にアクセスしないようにする。

○　ＯＳ等の脆弱性対策

利用している機器などの更新ファイル、パッチ等を適用して、脆弱性を残さない。

○　ウイルス対策ソフトの導入等によるマルウェア対策

ウイルス対策ソフトの定義ファイルを最新の状態に保つことで、感染するリスクを低減する。

○　認証情報の適切な管理

・　リモートデスクトップサービスや VPN 機器等の認証パスワードが脆弱だったため、ネットワークに侵入された事例も。

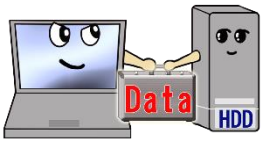
・　パスワードは、大文字・小文字・数字・記号の組み合わせにより、文字数が多く推測されにくい文字列を設定するとともに、他のサービスなどで使用していないものを設定する。

(2)　被害軽減対策

○　データのバックアップ

・　バックアップはなるべくこまめに取得し、ネットワークから切り離して保管。

・　日頃からバックアップデータによるシステムの復旧手順を確認。



○　アクセス権などの権限の最小化

ユーザーアカウントに割り当てる権限やアクセス可能範囲は必要最小限に。

これらの各種対策は、ランサムウェアのみならず、他のサイバー攻撃にも通じるものとなります。

多様化する脅威に備え、上記を含めた基本的な情報セキュリティ対策を徹底しましょう。

【出典：令和３年上半期におけるサイバー空間をめぐる脅威の情勢について（警察庁発行）】

【参考：警察庁ＨＰサイバー犯罪対策プロジェクト・ランサムウェア被害防止対策】

岐阜県警察